SafeNet HighAssurance 500/1000 Gateway Cryptographic Module

By SafeNet, Inc.

Security Policy
(Non-Proprietary)

FIPS140-2 Level-2 Validation
February 12, 2004

Document Version 1.01

Table of Contents

1 Introduction

1.1 Purpose

This is a non-Proprietary FIPS 140-2 Security Policy for the SafeNet HA500/1000 Gateway products. The Security Policy describes how the HA500/1000 meets all FIPS 140-2 Level 2 requirements, and was prepared as part of the HA500/1000's FIPS 140-2 certification submission package.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2) is a U.S. Government standard entitled *"Security Requirements for Cryptographic Modules*." This standard mandates a set of strict design and documentation requirements that hardware and software cryptographic modules must meet in order to be certified by the U.S. National Institute of Standards and Technology (NIST) and the Canadian Communications Security Establishment (CSE).

This document is intended for use by FIPS 140-2 testers, NIST and CSE reviewers, and others interested in how the HA500/1000 meets all FIPS 140-2 Level 2 requirements.

1.2 References

This FIPS 140-2 Security Policy describes features and designs of the HA500/1000 using the technical terms of FIPS 140-2.

- For more information on the FIPS 140-2 standard and validation program readers are referred to the NIST web site at http://csrc.nist.gov/cryptval/.

- For more information on the HA500/1000 product, please visit the SafeNet web site at http://www.safenet-inc.com.

1.3 Terminology

In this document the SafeNet HA500/1000 is referred to as the module, the HA500/1000 device, the device, and the HA500/1000.

1.4 Version History

Version	Date	Comments	Name
0.01	7/30/2003	Initial draft	Ward Rosenberry
0.02	8/13/2003	Second draft	Ward Rosenberry
0.03	8/20/2003	Submission draft	Ward Rosenberry
0.04	8/20/2003	Inc SafeNet Comments	Ward Rosenberry
0.05	9/10/2003	Inc COACT comments on v0.04	Ward Rosenberry
0.06	9/12/03	Inc Coact/SafeNet comments on v0.05	Ward Rosenberry
0.07	9/29/03	Inc Coact comments on v0.06	Ward Rosenberry
0.08	10/02/03	Finalized	Adam Bell
0.09	10/21/03	Updates as per initial consistency review	Adam Bell
1.00	2/5/04	Updates per NIST comments	Adam Bell
1.01	2/12/04	Final	Adam Bell

1.5 Acronyms and Abbreviations

ANSI American National Standards Institute

API	Application Programming Interface
CA	Certificate Authority
CC	Configuration Certificate
CBC	Cipher Block Chaining
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communication Commission
FIPS	Federal Information Processing Standard
FIPS 46-3	Data Encryption Standard (DES)
GUI	Graphical User Interface
HA500	High Assurance 500 Gateway
HA1000	High Assurance 1000 Gateway
HMAC	Keyed-Hash Message Authentication Code
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
KAT	Known Answer Test
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MAC	Message Authentication Code
MD5	Message Digest version 5
NC	Network Certificate
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
PRNG	Pseudo Random Number Generator
PUB	Publication
RAM	Random Access Memory
ROM	Read Only Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman Algorithm
SA	Security Association
SHA	Secure Hash Algorithm
SMC	Security Management Console
SNMPv2	Simple Network Management Protocol version 2
SRDI	Security Related Data Item
SSH	Secure Shell
SSL	Secure Sockets Layer
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security

VPN	Virtual Private Network
WLAN	Wireless Local Area Network

2 HighAssurance 500/1000 Gateway

The SafeNet HA500/1000 Gateway is a high-performance, standards-based hardware Virtual Private Network (VPN) and firewall. Providing a high speed, low cost solution, it features the strongest cryptography available and complete manageability. SafeNet custom designed a state-of-the-art Application Specific Integrated Circuits (ASIC) for the HA500/1000 that allows encryption using either AES, DES (legacy systems only), or triple-DES as needed by client applications.

The HA500 Gateway and HA1000 Gateway are identical in circuitry and software. They differ only in product name (and labeling) and by a factory set configuration parameter that defines the number of VPN tunnels that can be established at a given time.

The HA500/1000 supports the internationally standardized Internet Protocol Security (IPSec) protocol and Internet Key Exchange (IKE) protocol. Whether securing an enterprise perimeter, a corporate sub-network, or a single host, the HA500/1000 controls network access and gives administrators a complete toolbox of functionality. The HA500/1000 includes the following features:

- IPSEC support including IKE (using all modes – main, aggressive, and quick)
- X.509 v3 Digital Certificates, Public Key Infrastructure Certificate Management Protocol (PKIX CMP), and pre-shared keys
- Strong cryptography using AES, Triple-DES, SHA-1, RSA and DSA (Digital Signature Algorithm) signing. DES is included for legacy system support only. DSA is used for authentication only.
- Tamper-response/evident case.
- Encryption to enforce policy and provide data privacy
- Centralized, remote management using SNMPv2 and Telnet (remote management protected by a VPN tunnel).
- Local Management using an RS-232 CLI terminal interface.
- Secure automated software upgrades and security policy updates

The HA500/1000 acts as a perimeter guard. The module allows you to create enterprise-wide Virtual Private Networks and to securely link distributed networks by adding a single device in front of the network.

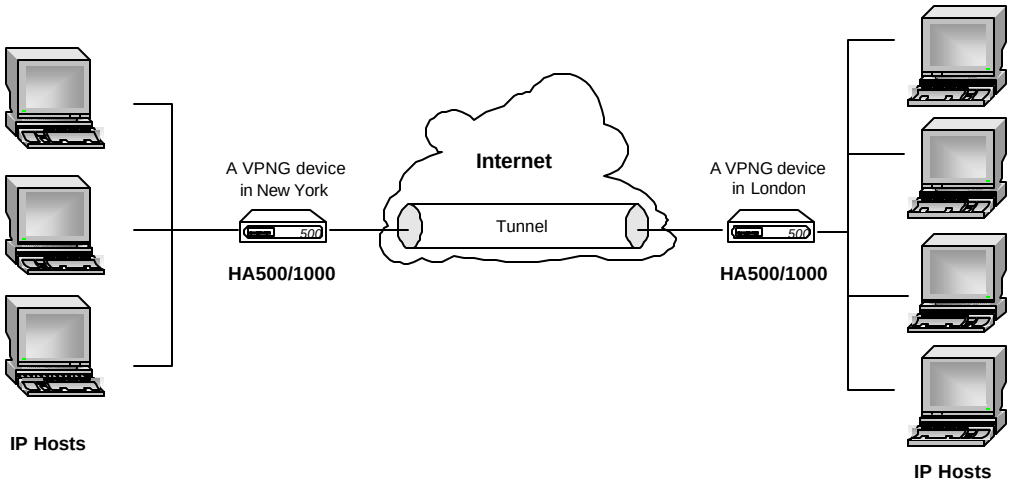

Figure 1 – HA500/1000 Securely Links Remote Networks

The possible authentication interactions are:

1. HA500/1000 to HA500/1000
2. SMC to HA500/1000
3. Other gateways (SafeNet and non-SafeNet) to HA500/1000
4. Software client (SafeNet and non-SafeNet) to HA500/1000

2.1 Secure Remote Management Software

The Security Management Console (SMC) is powerful remote management software that can be installed on an, Windows 2000, Windows XP, or Solaris 8.00 workstation. This software provides a simple, easy-to-use graphical interface to the configurations of the HA500/1000. It also allows for extensive monitoring of the HA500/1000, allowing an Administrator to remotely keep track of the module's status. All communications between SMC and the HA500/1000 are through network ports over secure, authenticated IPSEC tunnels. The SNMPv2 protocol and Telnet protocol are used to carry out the management services.

3 Security Levels

The HA500/1000 has been evaluated as meeting all FIPS 140-2 requirements at level 2 or higher security. Individual security requirements meet the levels indicated in Table 1.

Security Requirements Section	Level
Cryptographic Module	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self Tests	2
Design Assurance	2
Mitigation of other attacks	N/A

Table 1. Security Levels

4 Cryptographic Module Specification

In FIPS terms, the HA500/1000 Gateway is a multi-chip standalone module. The HA500/1000 features strong physical security including tamper response circuitry, a tamper-evident case, extruded sheet metal construction, and a SafeNet iridescent sticker. The entire module is encapsulated by the steel case that forms the cryptographic boundary, and only specified physical interfaces provide access to the module.

The HA500/1000 Gateway consists of the following parts:

- Hardware Assembly Part Number SE-HA500-01; (for HA1000) SE-HA1000-01.
- SafeXcel 1141/1741 encryption chip.

- System firmware includes the operating system, boot code and runtime firmware installed in ROM (flash memory) as part of the manufacturing process. Firmware consists of:
  - Boot Code Version 05.01
  - Runtime Version 05.01
  - SafeNet OS Version 05.01

A crypto officer (an administrator configuring or using the cryptographic module) can examine the product label to confirm the hardware assembly version number. The versions of firmware can be obtained by using the Show Version command that is available to crypto officers (administrators) of the cryptographic module. This allows the crypto-officer to verify the versions of the OS, boot code and run-time code match that of the FIPS 140-2 certified module. Figure 2 shows a hardware block diagram of the cryptographic module and indicates the cryptographic boundary.

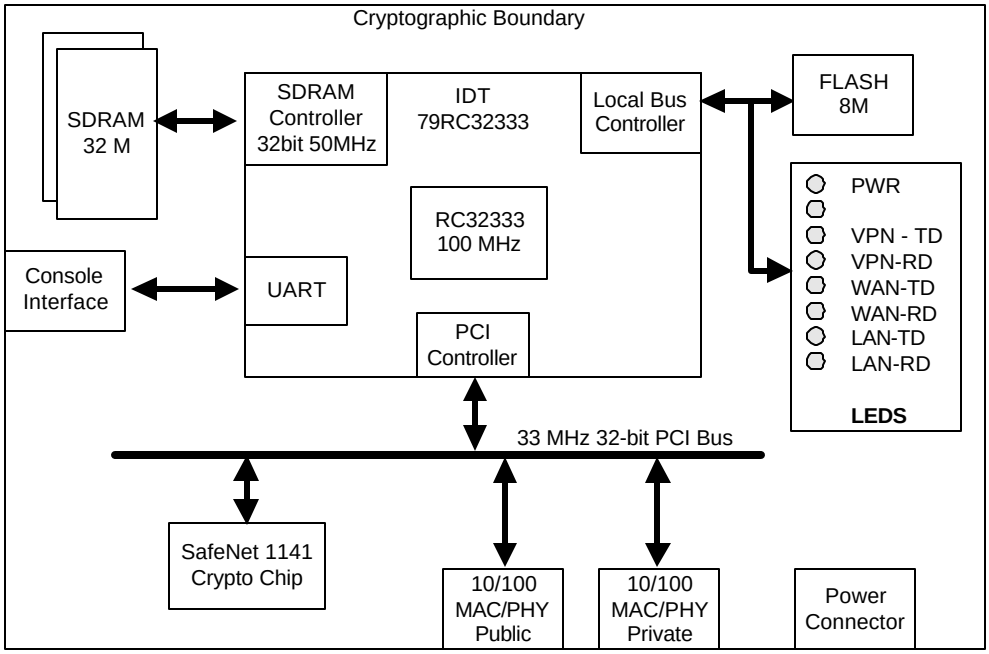

Figure 2 – HA500/1000 Block Diagram and Cryptographic Boundary

The module uses standard, production-quality components, designed to meet commercial-grade specifications for power, temperature, reliability, shock and vibration.

The HA500/1000 has tamper-evident security tape on the two screws securing the chassis housing that must be removed to access any internal cryptographic module components. A microswitch attached to the chassis senses any attempt to open the module. While the HA500/1000 is turned on, if an attempt to remove the module cover is detected the system responds by zeroizing any keys or Critical Security Parameters (CSPs) in flash memory (ROM) and disabling data traffic. While powered off, if the chassis cover is even partially removed, the module will detect the tamper upon the next boot cycle and will not support any cryptographic processes. Tamper evidence for the HA500/1000 includes dents and scratches in the metallic case, damage to the security tape, and severe deformation of any panels.

System timing controls and standard memory management design techniques prevent all operators and executing processes from modifying executing cryptographic processes such as

loaded and executing cryptographic program images. Timing controls and operating system access controls prevent operators and executing processes from reading cryptographic software stored within the cryptographic boundary. The SafeNet Operating System event log records record modifications, accesses, deletions, and additions of cryptographic data and CSPs.

Figure 3 – The Steel-Cased HA500/1000 Features Tamper Response Circuitry

4.1 Operational Environment

The cryptographic module has a limited non-modifiable operational environment consisting of the SafeNet OS. The physical embodiment is a multichip standalone module.

4.2 Module Interfaces

Table 2 shows the mapping of the FIPS140-2 logical interfaces to the module's physical interfaces.

FIPS 140-2 Logical Interfaces	Physical Interfaces
Data Input Interface	Private/Public Ethernet ports
Data Output Interface	Private/Public Ethernet ports
Control Input Interface	Private/Public Ethernet ports, Serial port, reset switch DC power connector
Status Output Interface	Private/Public Ethernet ports, Serial port, Front Panel LEDs
Power Interface	DC power connector

Table 2. Logical to Physical Interface Mappings.

The HA500/1000 has status indicators on the front panel that allow quick and easy assessment of the working condition of the module. These indicators show traffic through the module and if the power is connected. Policy indicators show when user traffic is passing in the clear, blocked or is being encrypted. Figure 4 and 5 depict the front/rear panel of the module. There is also a standard serial port for local configuration.

Figure 4 – Indicators Show The Status Of The Device

The HA500/1000 provides 10/100BaseT Ethernet Ports that allow it to plug directly into an existing network.

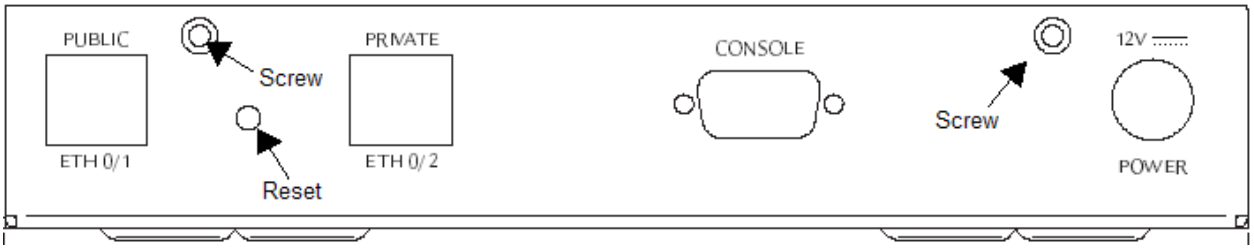

Figure 5 – Standard Interfaces Plug Directly Into Your Network

As shown in Figure 5 above, the private and public Ethernet ports (10/100baseT) are on the rear panel of the HA500/1000. There is also a standard RS232 serial console port for local configuration. Local management and monitoring services are available through the console port. However, using the secure SMC management station, an administrator can conveniently and remotely access and modify all configurations of the HA500/1000 through the Ethernet ports. Secured IPSec connections allow administrators to securely monitor and administer the HA500/1000 from remote locations.

The reset button provides three separate functions:

- Pressing the reset button for 5 seconds resets the speed of the console to 9600 bps and restores the private IP address to 10.10.10.1
- Pressing the reset button for 30 seconds triggers the following sequence of events:
  - Startup.cfg (containing current configuration settings) is erased from the file system
  - Manufacturing.cfg (containing default configuration settings) is copied to startup.cfg
  - The unit reboots.
- Holding down the reset button while the unit is booting causes the module to ignore the startup.cfg file on booting and to use the manufacturing configuration for this boot session. The next boot uses the normal startup configuration

To reboot the module using the current configuration, cycle the power.

4.3 Supply Voltage and Current

The HA500/1000 draws 12 VDC at 800 mA. Figure 6 shows the power connector

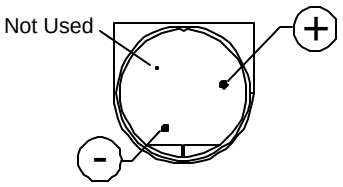

Figure 6 – Power Connector Pin Descriptions

4.4 EMI/EMC

The module meets FCC requirements in 47 CFR Part 15 for personal computers and peripherals designated for home use (Class B), and is labeled in accordance with FCC requirements.

4.5 Roles and Services

The HA500/1000 uses role-based authentication to provide access to cryptographic module services.

4.5.1 Roles

The HA500/1000 employs role-based authentication of its operators and supports two roles: crypto officer and user.

The **crypto officer** role is responsible for the configuration and management of the HA500/1000. The local crypto officer interfaces with the HA500/1000 through the local console port using the command line interface (CLI) or by using telnet (and the CLI) through the private Ethernet port. A remote crypto officer interfaces with the HA500/1000 through an IPSec-secured public Ethernet port using the SafeNet Management Console (SMC).

The local crypto officer has three capabilities in addition to those provided to remote crypto officers. These additional local crypto officer capabilities include:

- Initial configuration and secure setup of the HA500/1000.
- Enabling and disabling remote crypto officer access. Remote crypto officer access is initially disabled.
- Use of the ENG password to perform low-level functions on the HA500/1000. Low-level functions that alter the cryptographic module configuration violate FIPS compliance. The ENG (engineering) password is for emergency use only. It is not delivered with the module but can be obtained only by contacting SafeNet.

Note that local crypto officers do not use secure IPSEC sessions to communicate with the cryptographic module so they do not generate, use, or destroy cryptographic keys consisting of Diffie-Hellman keys, RSA asymmetric keys, or AES, TDES, or DES symmetric keys.

4.5.2 Crypto Officer Authentication

A local crypto officer authenticates using the crypto officer password. A default crypto officer password is available for initially configuring the HA500/1000. In FIPS mode, this password must be changed when initialization completes.

A remote crypto officer (using the SMC software) initially authenticates to the module using the pre-shared key and then using the crypto officer password. Once authenticated, the remote crypto officer generates an RSA public/private keypair and exports the public key as a PKCS#10 certificate request. A CA issues a public key certificate which is then loaded into the module and subsequently distributed to other IPsec devices as needed. All subsequent management sessions use RSA signatures for authentication within the IKE protocol as well as the crypto officer password before cryptographic module services are offered to the remote crypto officer.

4.5.3 Crypto Officer Services

Except for the three cryptographic module services provided only to local crypto officers (described in Section 4.5.1), the cryptographic module offers the following cryptographic services to remote crypto officers:

- RSA/DSA key generation
- RSA/DSA signature generation
- Diffie-Hellman key agreement
- DES, TDES, AES encryption and decryption (DES allowed for legacy support only)

The above cryptographic services are provided as part of IPSEC and IKE protocols.

Other services available to crypto officers include:

- Self-test
- Show Status
- Firmware update
- Hashing
- MACing
- Key Zeroization

The HA500/1000 Command Reference specifies all of the commands available to local and remote crypto officers to perform the above services.

4.5.4 User Authentication and Services

Any device initiating a valid IKE session is considered a legitimate user of the cryptographic module. Users are authenticated using RSA/DSA or by a pre-shared key.

Users can access the following cryptographic module services.

- **DH Key Agreement** – This cryptographic module service is used whenever a user initiates an IKE session with the module.
- **Symmetric key (AES, DES, TDES) Generation** – This cryptographic module service is used whenever a user initiates an IKE session with the module. An IKE policy module shared between the cryptographic module and the user dictates which key (AES, DES, TDES) to generate within the Diffie-Hellman key agreement protocol.
- **Encryption and Decryption services using AES, DES, TDES** – This cryptographic module service is used whenever a user communicates via the cryptographic module. An IKE policy shared between the cryptographic module and the user dictates which algorithm (AES, DES, TDES) is used.

- **Message Authentication Code** – – This cryptographic module service is used to authenticate clear text and cipher text messages.

4.5.5 Separation of Roles and Services

The module allows multiple concurrent operators consisting of multiple crypto officers and multiple users. Role separation is achieved by requiring each crypto officer to authenticate to the module. System timing controls and standard memory management techniques isolate concurrent management sessions from one another. The IKE and IPSec protocols isolate concurrent user sessions from one another.

4.6 Cryptographic Algorithms, Security Functions and Key Management

Always adhering to the cryptographic standards, HA500/1000 provides the strongest cryptography available. HA500/1000 supports IPSEC/ESP data encryption, IPSEC/ESP data integrity (with the prescribed NULL encryption algorithm), and IPSEC/AH for data integrity in Tunnel mode. HA500/1000 implements all IKE modes: main, aggressive, and quick, using ISAKMP. The HA500/1000, with the following algorithms, supports these features:

Data Encryption

- AES-CBC (256 bits, 192 bits, 128 bits) – as per NIST FIPS PUB 197
- Triple DES-CBC (168 bits) – as per NIST FIPS PUB 46-3
- DES-CBC (56 bits) – as per NIST FIPS PUB 46-3 (for legacy support only)

Data Packet Integrity

- HMAC-SHA1 (20 byte) – as per NIST FIPS PUB 198

Random Number Generation

- Non-Deterministic Random Number Generator (NDRNG) implemented in hardware.

Authentication

- RSA – vendor affirmed to PKCS#1
- DSA – vendor affirmed (no certificate) to FIPS PUB 186-2
- All IKE modes – main, aggressive, and quick modes
- Password authentication in accordance with FIPS PUB 140-2.
- Pre-shared key (Authentication for initial configuration and VPN tunnel authentication.)

The HA500/1000 implements cryptographic keys and CSPs which are generated, stored, used and destroyed in accordance with FIPS 140-2 as described in Table 3.

Table 3. Cryptographic Key and CSP Generation Use and Destruction.

Pre-shared key	This is the default human readable string used only to authenticate the first remote crypto officer management session is not used thereafter. Its use is described in the installation and configuration documentation.
IKE pre-shared key	Used to authenticate users in IKE. Electronically entered into the module from SMC over a secure IPsec tunnel.
RSA/DSA public/private key pair	This is a persistent RSA/DSA public key set generated by the cryptographic module during the first remote crypto officer management session. The public key is exported to a CA; the certificate is imported and stored in clear text form in flash. The private key is stored in clear text form in flash. The key pair is used to authenticate remote crypto officer management & user sessions. The private key and the corresponding certificate are erased during tamper response.
1 crypto officer password	This is an 8 byte password that can include any type-able characters (A-Z,a-z,0-9 and punctuation including space characters but not the TAB). It may be set by the local crypto officer for Remote and Local crypto officer access. The crypto officer password is stored as an MD5 hash in flash memory.
1 ENG password	This is an 8 byte password that can include any type-able characters (A-Z,a-z,0-9 and punctuation including space characters but not the TAB) set by the *manufacturer* for emergency Local crypto officer access to low-level functions like updating boot code or removing files from the system. The password is stored within the code image. The ENG password can be obtained solely from the HA500/1000 manufacturer.
DH keypairs	Public/private Diffie Hellman keypairs are generated dynamically per-security association, and used in RAM (in the clear) for the IKE (Internet Key Exchange) phase of IPSEC to establish a shared secret key (DES, TDES, or AES). When DH key agreement completes, the DH private key is no longer useful. It remains in RAM until it is zeroized on reset.
DES, TDES, or AES session keys	An ephemeral symmetric key, derived from DH key agreement, stored in RAM, and used for session encryption of payload traffic between endpoints. Each security association has a unique DES, TDES, or AES key to provide confidentiality to the payload traffic from other users in the system. During use, the key is stored in RAM. When the session completes or on re-key (sessions can be set for automatic re-key after a given time limit, a specific amount of data has been transferred, authenticated request from a remote user or request from a remote crypto officer), the key is no longer useful and is zeroized on reset. Session keys are erased from RAM during tamper response.
HMAC Authentication keys	The authentication key is stored in RAM and used for message integrity. When the session completes or on re-key (sessions can be set for automatic re-key after a given time limit, a specific amount of data has been transferred, authenticated request from a remote user or request from a

	remote crypto officer), the authentication keys are no longer useful and are erased from RAM. The specific key is decided during IKE and can be used for HMAC SHA-1 and HMAC MD5. Authentication keys are erased from RAM during tamper response.

4.6.1 Other Security Functions

The HA500/1000 does not provide any other security functions.

4.7 Self-Tests

The HA500/1000 monitors firmware operations through a set of self-tests to ensure proper operation in accordance with FIPS 140-2. The module includes the following power-up self-tests and conditional tests.

4.7.1 Power-Up Self-Test

The power-up self-test includes the following tests:

Hardware Tests: When power is first applied to the module, the hardware performs a series of checks to ensure it is functioning properly.
Firmware Software Integrity Test: The module performs SHA-1 check value verification to ensure the firmware and software modules have not been modified. The length of the hash is 20 bytes. If the resultant hash value does not match the stored value, the test fails and the module enters the self test error state.
NDRNG Functional Test – a functional test of the non-deterministic random number generator is run during power up as a critical function test.
Cryptographic Algorithm KATs: Known Answer Tests (KATs) are run at power-up. KATs input known strings into cryptographic algorithms so that the expected output is known. If the expected output does not match the actual algorithm output, the test fails. The module supports the following KATs:

DES-CBC KAT (Encrypt &Decrypt)
Triple-DES-CBC KAT (Encrypt & Decrypt)
AES-CBC KAT (Encrypt & Decrypt)
HMAC-SHA-1 KAT
DSA KAT
RSA KAT

If all of the power-on self tests pass, the module is ready for use by operators. If any test fails, an error message indicating which test failed is output to the status output interface (the CLI). In this case the module enters an error state and no cryptographic operations can be performed. The module must be rebooted or reset to a factory-default state to clear this error.

Local crypto officers can perform the self test on-demand by cycling the module power. During boot (during self test), the LEDs do a pattern walk from right to left. If the self test fails, the STATUS LED turns RED,and the crypto officer can check the CLI for the specific error (this action is equivalent to a SHOW STATUS service). If the test passes, the LEDs assume normal operation wherein the Power LED is lit and the VPN, WAN and LAN LEDs light as needed.

A remote crypto officer can perform the self test on-demand by issuing a reload command. If the self test fails, a remote crypto officer can not communicate with the device (after the usual reboot period) and this symptom indicates that self-test has failed. In this case, only a local power cycle

is possible to reboot the module. If the self test passes the remote crypto officer can establish a new management session.

Note that on a power recycling or reload command, any services in use are stopped. After reboot, new management sessions and IKE sessions must be established.

4.7.2 Conditional Tests

DSA Pair-wise Consistency Test: DSA operations are tested to ensure the correct operation of the DSA key generation, signatures, and SHA-1 hashing algorithms.
RSA Pair-wise Consistency Test: RSA operations are tested to ensure the correct operation of the RSA key generation, signatures, and SHA-1 hashing algorithms.
Continuous Random Number Generator Test: This test is constantly run to detect failure of the random number generators in the HA500/1000
Firmware Upgrade Test: The Module's entire firmware can only be remotely upgraded from the management system with proper authentication to the module. The integrity of the new firmware is guaranteed by a SHA-1 hash.

If the conditional tests pass, the module remains ready for use by operators. If any test fails, an error message indicating which test failed is output to the status output interface (the CLI). In this case the module enters an error state and no cryptographic operations can be performed. The module must be rebooted to clear this error.

5 FIPS 140-2 Mode

When properly configured, the HA500/1000 always operates in a FIPS 140-2 compliant manner for level 2 when the power-up sequence completes successfully.

The Crypto Officer Guidance provides instructions that must be followed to ensure the proper configuration for FIPS mode operations. If all of the Crypto Officer Guidance has been performed and the Power-up sequence executes successfully, the crypto officer can be assured the module is operating in FIPS mode.

In FIPS mode the following FIPS-approved cryptographic algorithms may be used:

Data Encryption

- DES-CBC (56 bits) – Cert. #233 as per NIST FIPS PUB 46-3 (for legacy compatibility only)
- Triple DES-CBC (168 bits) –Cert. #210 as per NIST FIPS PUB 46-3
- AES-CBC (256 bits) – Cert #96 as per NIST FIPS PUB 197

Data Integrity

- HMAC-SHA-1 (20 byte) – Cert. #187; vendor affirmed as per NIST FIPS PUB 198
- SHA-1 (20 byte) – Cert #187 as per NIST FIPS PUB 198

Authentication

- RSA – vendor affirmed to PKCS#1
- DSA – as per NIST FIPS PUB 186-2 (no certificate)

Key Agreement

- Diffie Hellman – vendor affirmed to PKCS#3

All traffic employing encryption and/or authentication must be encrypted using AES, DES or Triple-DES and authenticated using RSA signatures or IKE pre-shared keys.

The SafeNet tamper-evident stickers must be affixed to the HA500/1000 under normal operating temperatures, and the surface for application of the stickers must be clean and dry.

6 FIPS 140-2 Level 2 Non-Compliant Mode

The module may operate in non-FIPS mode if a crypto officer modifies the module configuration in any way. Examples of module reconfiguration include:

- Setting a weak crypto officer password.
- Using the ENG password to modify the flash file system. This includes upgrading the BOOT image.
- Specifying the use of HMAC-MD5 when generating Message Authentication Codes (MACs) when performing message authentication.
- Specifying "NULL" for the encryption algorithm in ESP

Crypto officers must avoid reconfiguring the module such that it is no longer FIPS compliant. Reconfiguration includes removing files, updating the firmware, and opening the chassis such that the tamper evident tape shows signs of tampering.

In non-FIPS mode, the module may use the following algorithms:

Data Integrity

- HMAC-MD5 (20 byte) – as per FIPS PUB 198

7 Security Rules

7.1 Identification & Authentication Security Rules

The module implements specific methods for identifying and authenticating the different roles. The implementation consists of the binding of a Role-Based Access Control Rule to each service.

7.1.1 Cryptographic Officer Identification and Authentication

A crypto officer using the CLI (through the local console port or using telnet through the private Ethernet interface) must prove possession of the crypto officer password. A valid password causes the module to allow local crypto-officer access to services. A crypto officer using SMC through the private or public Ethernet interface must authenticate using RSA public key authentication and then prove possession of the crypto officer password. These two actions cause the module to allow remote crypto officer access to services.

Role	Type of Authentication	Authentication Data
Remote crypto-officer	Certificate + password	Signature based on 1024 bit key and

		String of length 8
Local crypto-officer	Password	String of length 8
User	Certificate or pre-shared key	Signature based on 1024 bit key String of length 8

Table 4. Roles and required identification and authentication

7.1.2 User Identification and Authentication

A user authenticates to the module by conducting a valid IKE session with the module. Thus, any user conducting and completing a valid IKE session is considered an authenticated user of the module. The IKE protocol uses dynamically generated Diffie-Hellman keys and the Diffie-Hellman key agreement protocol to negotiate a symmetric key that is shared between the user and the cryptographic module. All subsequent session communications use the negotiated keys for confidentiality and authentication.

7.2 Reauthentication After a Power Cycle

If power is removed and re-applied to the module, any active crypto officer management sessions and any user sessions are terminated. Crypto officers must reauthenticate to access protected services offered by the module and users must initiate valid IKE sessions to receive any cryptographic services.

7.3 Strength of Authentication

Only crypto officers authenticate to the cryptographic module using the following authentication methods:

- crypto officer password authentication
- Pre-shared key authentication
- RSA/DSA authentication

Peers (users) authenticate using user pre-shared key authentication.

The strength of the each authentication mechanism is explained in Table 5 and the following sections.

Table 5. Strength of Each Authentication Mechanism.

Authentication Mechanism	Strength of Mechanism	Chance of guessing attempts per minute
Crypto officer password	$>62^8 = 2.18 \times 10^{14}$	$>2.78 \times 10^9$
Pre-shared key authentication	$68^6 = 9.88 \times 10^{10}$	1,260,059
IKE Pre-shared key	$68^6 = 9.88 \times 10^{10}$	1,260,059

authentication		
RSA/DSA certificate (1024)	10^{28}	1.66×10^{24}

7.3.1 Crypto Officer Password Strength

The minimum length of the crypto officer password is 8 bytes. Each byte of the password can be one of the characters a-z, A-Z, 0-9, and certain other characters, yielding a greater than1 in 62^8 = 2.18×10^{14} chance of guessing the password.

To try an 8-byte password, an attacker must send a 8 bytes to the module and get a resulting 2 byte response. As there is a single I/O port on the platform, this means that each PIN attempt requires 10 bytes of data to be clocked in or out of the module. The maximum data rate for the module is 9600 bps through this single port. If we ignore the processing time required on the module to check the password, we can compute the maximum number of password attempts that could occur within a 60 second interval:

- 10 bytes of I/O * 8bits/byte = 80bits/attempt
- 9600 bits/second * 1 attempt/88bits = 109 attempt/second
- 60seconds/minute * 109 attempts/minute = 6540 attempts/minute maximum

The chance of guessing a ROM password is 1 in 3.33×10^{10} per minute. This exceeds 1 in 100,000 per the requirement.

When the password authentication is attempted over the telnet session via the Ethernet interface the attempt rate is much faster. Upon 3 consecutive failures to login in to the module, the CLI will stop responding for 3 seconds. Therefore a maximum of 20 attempts per second is enforced.

The chance of guessing a password is 1 in 1.0×10^{13} per minute. This exceeds 1 in 100,000 per the requirement.

Feedback of authentication data to an operator is obscured during authentication. Neither the CLI nor the SMC returns a visible display of characters when entering a password.

7.3.2 Pre-Shared Key Strength

The minimum length for a pre-shared key used to authenticate the crypto officer is 8 bytes. This is a fixed value for the first authentication between the module and the crypto officer. Each byte of the password can be one of the characters a-z, A-Z, 0-9, yielding a 1 in $62^8 = 2.18 \times 10^{14}$ chance of guessing the pre-shared key.

The IKE process can allow for 1 IKE attempt from a defined peer IP address and Port. At best, an attacker could attempt 10,000 concurrent authentications. The IKE process is no faster than 1 second to complete. The chance of guessing the pre-shared key in one minute is

$$2.18 \times 10^{14} / 60{,}000 = 3.63 \times 10^{9}$$

Therefore the module far exceeds the requirement of 1 in 100,000 for multiple attempts in a 60 second interval.

7.3.3 IKE Pre-Shared Key Strength

This has the same strength as the pre-shared key (See Section 7.3.2 Pre-Shared Key Strength).

7.3.4 RSA/DSA Authentication Strength

Crypto officers must authenticate to the module using an RSA/DSA key of 1024 bits. This key space allows 2^{1024} values which require significantly more attempts than one million to guess the correct key. At most, 60,000 IKE sessions can be requested in a one minute interval resulting in a 1 in 2^{1024}/60,000 or 1 in $3x10^{303}$ false acceptance rate per minute.

7.4 Software and Firmware Loading Security Rules

The cryptographic module allows only loading of FIPS validated software and firmware by reloading the entire flash ROM firmware and software image. A SHA-1 hash authenticates and integrity protects the loadable image.

7.5 Access Control Security Rules

Table 6 describes the type of access operators have with respect to various cryptographic keys and CSPs. Note that "execute" means to trigger the operation on the crypto module that uses the CSP.

Table 6. Cryptographic Key and CSP Access Control

Key or CSP	Local crypto officer	Remote crypto officer	User
Pre-shared key	no access allowed	read,	no access allowed
Pre-shared IKE key	no access allowed	read, write	read
RSA/DSA private key	read, write	execute	execute
1 crypto officer password	write, read	write, read	no access allowed
1 ENG password	no access allowed	no access allowed	no access allowed
DH private key	no access allowed	execute	execute
DES, TDES, or AES session keys	no access allowed	Execute, erase	execute

7.6 Physical Security Policy

The physical security of the cryptographic module meets FIPS 140-2 level 2 requirements. The module has security tape for physical protection during transfer and crypto officers are instructed to confirm the integrity of the module before initializing the module for use. Any attempt to gain physical access to the module will leave evidence of tampering. Crypto officers should examine the module periodically to check for evidence of tampering such as dents, scratches or damaged security tape.

A tamper switch detects any attempt to open the cryptographic module, zeroizing CSPs and disabling data traffic. If a crypto officer detects tampering, the crypto officer should notify the organization's security officer.

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Security Tape	As per direction of security officer	If tape is damaged disconnect Ethernet cables and contact the security officer.
Signs of Physical damage	As per direction of security officer	If the enclosure shows new dents or scratches, disconnect Ethernet cables and contact the security officer.
Tamper-response circuitry	N/A	If the tamper response circuitry is activated, disconnect Ethernet cables and contact the security officer.

Table 7. Inspection/Testing of Physical Security Mechanisms

7.7 Key Management Security Policy

7.7.1 Cryptographic Key Generation

- DES Session key derivation as per PKCS#3 and FIPS PUB 46-3
- TDES Session key derivation as per PKCS#3 and FIPS PUB 46-3
- AES Session key derivation as per PKCS#3 and FIPS PUB 197
- DH key pair generation as per PKCS#3
- RSA key pair generation as per PKCS#1.
- DSA key pair generation as per FIPS PUB186-2.
- HMAC key generation per FIPS PUB 198.

No intermediate key generation values are output from the cryptographic module upon completion of the key generation process.

7.7.2 Cryptographic Key Entry/Output

No keys are manually input into the module.

7.7.3 Cryptographic Key Storage

The RSA private keys are stored in the clear in protected and hidden files in flash ROM. The cryptographic module's Roles and Services mechanism correctly associates keys with their correct entity.

7.7.4 Cryptographic Key Destruction

There are two commands that will cause key destruction:

No crypto ike sa
This causes the IKE phase 1 SAs (keys and IVs) to be erased.

No crypto ipsec sa
This causes the IPSec phase 2 SAs (keys and IVs) to be erased.

If the module is opened such that the tamper switch is activated, the module will reset and will continue to reset until the tamper condition is removed. This is fully described in the Finite State Machine document.

The following steps are executed upon a power up cycle after a tamper condition was discovered (and previous active tamper condition was removed)

- Zeroize RAM
- Zeroize the CSPs stored in Flash except the default pre-shared key
- Copy tamper.cfg to startup.cfg
- Load software

All VPN communications are immediately halted and any DES, TDES or AES keys in RAM are zeroized.

If the reset button on the back of the unit is depressed for 30 seconds the module will return to the default manufacturing settings, zeroizing any CSPs held in flash memory.

The cryptographic module cannot re-enter FIPS-approved mode until a remote crypto officer reinitializes the box using the default pre-shared key.

APPENDIX A — HA500/1000 Services

For a complete list of all commands available to crypto officers using the CLI, refer to the HA500/1000 Command Reference document. For a complete list of commands when using the SMC, refer to the SMC User's Guide.